ProTech *"Charting the Course ...*

protechtraining.com

*... to Your Success!"*

# Network Traffic Analysis

# Course Summary

**Description**

Grow Your Analytic Intelligence.

Network Traffic Analysis will enable students to differentiate between normal and abnormal network traffic. The course focuses on research, filtering, and comparative analysis to identify different types of activity on a network and attribute their source. A subject matter expert will teach you security-related tactics, techniques, and procedures for performing network analysis in today's ever-changing threat landscape. You'll learn to follow conversations through redirection, as well as how to develop custom filters for non-dissected protocols. After completing this course, students will be able to hone in on the key events in a traffic capture and reconstruct the event time line.

Using the tools, skills, and methodologies taught in Days 1 through 4 of the class, on Day 5, students will participate in a competitive capture-the-flag exercise. Designed to challenge the participants, each correctly completed milestone will unlock a successively more difficult challenge.

**Objectives**

After taking this course, students will be able to understand:

- Internet-Based Open Source Research
- Wireshark Protocol Analyzer
- Effective Capture and Display Filtering
- Tracing System, Service and User Transactions
- Recognizing Encoding Types
- Base-64 and URL Encoding
- Non-Dissected Protocol Analysis
- HTTP Header Analytics (User-Agents, Referrers, Accept Lines, etc.)
- Cookie Tracking

**Topics**

- OSI & TCP/IP Models
- Number Theory
- Wireshark Tutorial
- Day in the life (TCP/IP)
- Analytic Process
- Internet Research
- Traffic Analysis
- Attribution
- Research Techniques
- Start-to-Finish Protocol Analysis
- Regular Expressions
- Analysis beyond Wireshark
- Security Protocols
- User Agents
- Cookies
- Analysis of a Big Capture File
- Tips and Tricks
- Student Practical Demonstration

**Audience**

This course is designed for:

- Network Analysts seeking to develop security-related skills
- Incident Responders needing to quickly address system security breaches
- Penetration Testers looking to reduce their detectability
- Threat Operations Analysts seeking a better understanding of network intrusions
- All Network Administrators needing a better understanding of network security

# Network Traffic Analysis

## Course Summary (cont'd)

**Prerequisites**

Before attending this course, student should have:

- A Broad Understanding of TCP/IP and Associated Protocols
- Knowledge of Network Hardware and Segment Types
- Previous exposure to Wireshark or other protocol analysis software is also recommended

**Duration**

Five days